Challenges for ensuring the information security of commercial banks

Bojidar Bojinov

Tsenov Academy of Economics, Svishtov, Bulgaria

2016

CHALLENGES FOR ENSURING THE INFORMATION SECURITY OF COMMERCIAL BANKS

Prof. Bojidar Bojinov, PhD

Tsenov Academy of Economics, Svishtov, Bulgaria

Abstract: The introduction of new information and communication technology into banking has radically altered the essence and character of banking activity. Alongside the competitive advantages and the direct economic effect of the advent of high-tech innovation in the banking sector, credit institutions are facing a number of challenges, one of them being to ensure the security of their products and related information. The main objective of this research is to elucidate the nature, instances, and methods of managing data security in commercial banks. An emphasis is put on some sources of operational risk in commercial banks which have a direct impact on the potentially growing risk in terms of data security. The research also focuses on the role of bank management in governing that process, as well as the methods and mechanisms for reducing the occurrence of the risk related to information security.

Key words: banks, data security, information technology, distance banking, online banking.

JEL: G21.

INTRODUCTION

The advent of new information and communication technology in banking has gradually, yet radically altered the essence and character of banking activity. From a historical perspective, the adoption of innovative communication methods has helped reduce price differentials in geographically distant markets. In terms of organization, technological innovations have contributed to the more efficient integration and communication between departments and to expanding the product range and distribution channels of retail banks.[1] Alongside the competitive advantages and the direct economic effect of the advent of high-tech innovation in the banking sector, credit institutions are facing a number of challenges, one of them being to ensure the security of their products and related information[2].

The main objective of this research is to elucidate the nature, instances, and methods of managing data security in commercial banks. Hence, the object of the research is data security of bank assets, while the

[1] See: Batiz-Lazo, B., Wood, D. Information technology innovations and commercial banking: a review and appraisal from an historical perspective. Accounting and finance research unit, Manchester Business School, The University of Manchester, 2001, ISBN 0 7492 45476, p. 3.

[2] Bank security is an instance of the commitment of banks to ensure the safe storage and management of customers' and banks' assets and related data, as well as to guarantee the physical security and safety of clients and employees in bank offices. Specialized dictionaries define the term 'security' as the 'physical security, internal audits, and prescribed procedures for ensuring the safety of customers and accounting records' and 'protection from attacks; confidentiality; warranty that deposited money will be paid back'. In economic literature, the term is generally approached as 'creating an environment in which dangerous conditions or circumstances are absent or their possible consequences are reduced to such a level that they would not be detrimental to the smooth functioning of a bank, its property, or infrastructure, or prevent banks from achieving their goals'; and protection from hazards related to the conscious actions of individuals or legal entities and designed to cause damage to a bank. See: Шишманов, К. Използването на съвременните информационни технологии в банковото дело – предизвикателства и реалност. Финансова стабилизация и икономически растеж. Сборник доклади, Свищов, 2000, с. 121; Fitch, T. Dictionary of Banking terms. Barrons's, 1997, p. 413; Dictionary of Banking and Finance. A&C Black Publishers Ltd, 2005, p. 319; Лаврушин, О.И. Банковский менеджмент. Москва, Кронус, 2009, с. 519; Алавердов А.Р. Организация и управление безопасностью в кредитно-финансовых организациях. Московская финансово-промышленная академия. Москва, 2004, с. 6.

subject focuses on available opportunities for efficiently managing that security.

* * *

There is no generally accepted definition or uniform approach to the essence and scope of data security in specialized literature[3]. Within a broader context, data security refers to all aspects of managing and preserving the integrity of the data processed by a particular entity, whatever the technical device used to store or process that data. Within the context of society computerization, the term 'data security' has acquired a narrower meaning to refer solely to the process of managing and ensuring the security of electronic data only. The scope of the concept has evolved, too, and from initially referring to the set of measures for protecting data from unauthorized access, nowadays it comprises the entire range of measures for preventing and dealing with problems in the operation of IT systems, alongside the measures adopted to protect information flows from unauthorized access or use.

At the same time, data security directly relates to the occurrence of operational risk in the banking sector[4] and is a direct consequence of operational problems, organizational changes, lack of or inadequate procedures, no segregation of duties, insufficiently or inadequately trained staff, internal control violations, fraud or unpredicted events which may result in contingent losses, errors, delays in the fulfilment of

[3] For further reading on issues related to general bank security, its varieties and forms, see: Божинов, Б. Банковата сигурност – основни проявления и аспекти. Народностопански архив, бр. 3, 2016.

[4] For further reading on issues related to bank risks, see: Божинов, Б. Управление на рисковете в търговската банка. Библиотека „Образование и наука", бр. 58, АИ „Ценов", Свищов, 2013.

tasks, IT system failures, fires and disasters which lead to the destruction of assets or data. [5]

The most common sources of operational risk which affect data security relate to: [6]

- *Staff (the human factor)*, and in particular:
  - *Inadvertent and/or incompetent actions* relating to lack of adequate skills and knowledge; inadequate training; lack of awareness about performance standards; employed methods, tools, and procedures; negligence; technical errors; inadequate control, etc.;
  - *Deliberate actions* related to unauthorized transacting; theft; forgery of data in the accounting system; forgery of financial and payment documents; theft of cash; hacking; breach of bank rules and procedures; money laundering; insider trading, and other intentional acts for the purpose of personal gain;
  - *Poor planning and management of personnel* – staff shortage and its replacement with insufficiently trained or qualified staff; sick leaves; staff turnover, etc.;
  - *Affecting customers' interests* through breach of bank secrecy; disclosure of personal and/or confidential information; damaging the interests of clients, etc.;
- *Internal processes* – breaches in prescribed rules, guidelines, processes, policies and control procedures; poor risk assessment and risk measurement in result of errors or omissions in applied models;

[5] See: Димитрова, Т. Вътрешният одит – ефективен инструмент на банковия мениджмънт, библиотека Образование и наука, бр. 38, АИ Ценов, Свищов, 2013, с. 87

[6] See further: Трифонова, С. Управление на операционния риск на банките. Вътрешен одитор, VII, N 1, 2010.

- *Systems* – problems in the IT systems which lead to a partial or complete interruption of bank operations. Those could be divided into:
  - *General systematic risks* related to restricted access to systems and networks; inadequate procedures for data backup and recovery; anti-virus and malware protection policy; policy on restricting unauthorized access to the systems, etc.;
  - *Risks related to the software used*, which may be due to system failures; errors in computation and/or reporting of operations and other programming errors in result of obsolete and/or inadequate technology; unauthorized access to customer data and accounts; data back-up problems, etc.;
  - *Risks related to the hardware*, which refer mainly to using out-dated or poor quality computer systems; lack of crucial backup servers and hardware items; lack of backup and recovery systems; lack of emergency power systems, etc.
- *External factors* related to:
  - *Force majeure* – disasters, fires, vandalism, terrorist attacks, etc.;
  - *Deliberate third-party actions* – robbery, fraud on behalf of the bank, hacker attacks, illegal access to customer accounts, other deliberate actions;
  - *Risks related to service providers* – providers of telephone services, power supply, telecommunications, outsourcing services, etc.

A specific feature of bank activity is *the confidentiality* requirement in terms of borrowed and managed funds and their owners, which relates directly to the trust-based relationship between banks and their customers. This is also one of the reasons why banks are extremely reluctant to disclose their problems, including any incidents and security breaches in their information systems. Such information generally leaks out only after a financial crime has been detected, through independent specialized institutions, or when intruders themselves publicly announce their breakthrough. [7] We should note that according to statistics *only 7 % of all bank crime is committed using computer and IT technology*. [8]

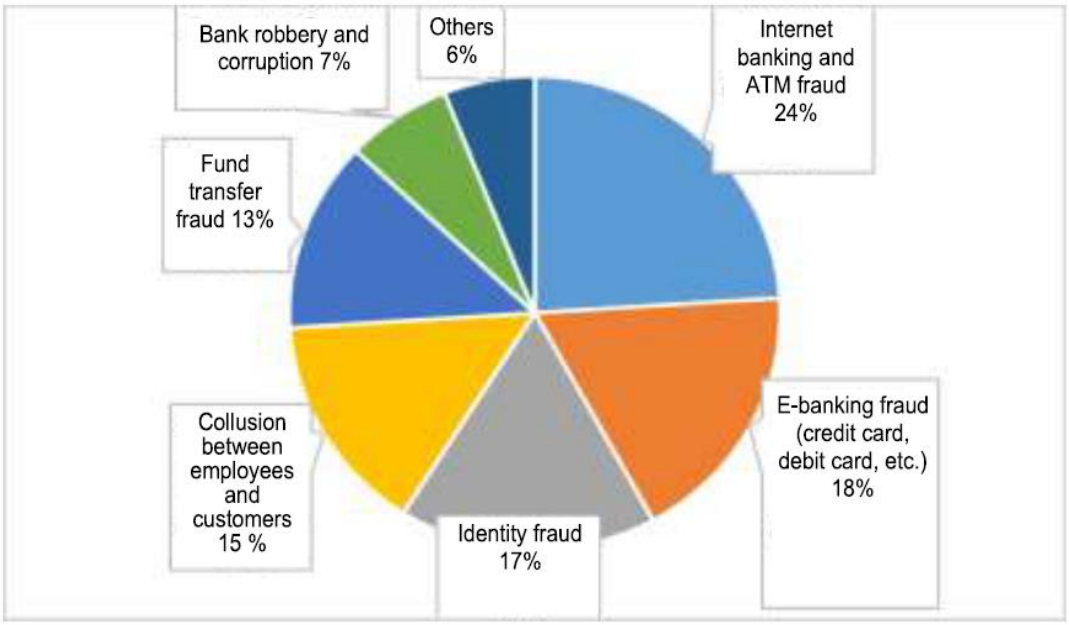

Fig. 1. Frequency of occurrence of major risks related to bank fraud [9]

[7] See: Хакери източили $71 млн. от банка през SWIFT. http://technews.bg/article-90580.html (last access 29.05.2016); Хакери атакуваха сайта на гръцката централна банка. http://news.bnt.bg/bg/a/khakeri-atakuvakha-sayta-na-grtskata-tsentralna-banka (last access 29.05.2016); Хакери са източвали средства от близо 100 банки по света. http://www.capital.bg/biznes/kompanii/2015/02/16/2473701_hakeri_sa_iztochvali_sredstva_ot_blizo_100_banki_po/ (last access 29.05.2016)

[8] See: Звезда, И.И. К вопросу о классификации способов мошенничества в банковской сфере. Известия Тульского государственного университета. Экономические и юридические науки, 2015, том 3-2, 97-105, с. 99.

[9] See: Deloitte - India Banking Fraud Survey - Edition II, 2015, p. 27.

Major attacks on the data security of bank systems through theft, manipulation, or destruction of data are an attempt either to get rich quickly or to cover or commit another crime. These relate mainly to: [10]

- *ID related fraud* committed to take over the accounts of third parties or to open accounts and acquire financial instruments through false identity. While the aim of the first type of crime is direct theft of cash, the second type of crime is generally part of a complex criminal scheme for committing commercial, financial, insurance, or tax fraud;
- *Acquiring confidential information to engage in various espionage activities*, in most cases to collect information about a business or a family partner, as well as to gain access to internal information which could be used for future enrichment;
- *Exploiting existing bank infrastructure to commit financial and tax crime*. In addition to financial, commercial, and tax fraud which involves the bank accounts of real and/or fictional persons and companies, organized crime also uses the bank system to conceal the true origin of funds acquired illegitimately and to facilitate their infiltration and integration into legal economy (a process known as 'money laundering'[11]);

[10] Adapted after: Lagazio, M., Sherif, N., Cushman, M. A multi-level Approach to understanding the Impact of Cyber Crime on the Financial Sector. p. 8.

[11] The term 'money laundering', which is used as an umbrella term for legitimizing ill-gotten gains, describes the practice of American mafia which used to filter in cash from gambling as earnings received from the laundromat business. Meyer Lansky, Al Capone's financial advisor, is believed to have been the first person to exploit the bank system for legitimizing earnings from criminal business during the Prohibition in the Unites States. See: Storm, A. Establishing The Link Between Money Laundering and Tax Evasion. The Clute Institute International Academic Conference Munich, Germany 2014, p. 1; Alacer. Happy Birthday, Anti Money Laundering! http://www.alacergroup.com/happy-birthday-anti-money-laundering/ (last access 11.6.2016).

- Cybercrimes[12] are in most cases designed to steal funds, yet they may be committed to conceal evidence of other crime by destroying all currently accessible or back-up data at a bank. Cyber terrorism and information warfare[13], despite having different origins and objectives, pose a serious threat to bank activity, too, since both aim to totally destroy data and IT infrastructure, to interrupt normal business processes, and to cause problems to banks, the financial system, and economy in general.

Fig. 2. Major impacts of data security problems upon bank institutions[14]

[12] Specialized literature distinguishes among several categories of cybercrime: traditional crime, hybrid cybercrime, true cybercrime, and cyber platform crime. Traditional cybercrime relates to exploiting cyberspace as providing more opportunity for crime (for example, traditional fraud, piracy, espionage, stalking, trading sexual material). Hybrid cybercrimes mainly relates to the activity of criminal groups which benefit from new opportunities provided by the Internet (such as ID theft, hacking, hacktivism, illegal online trade). True cybercrime relies on the opportunities created purely by the Internet and is carried out entirely within the cyberspace (for example, spam, denial of service, illicit cybersex). Cyber platform crimes (botnets, for instance) are committed to facilitate other types of crime, rather than to directly carry out criminal activity. See further: Lagazio, M., Sherif, N., Cushman, M. A multi-level approach to understanding the impact of cyber crime on the financial sector. p. 7.

[13] See: Кибертероризъм – заплаха отвъд виртуалното пространство. http://news.unabg.org/ кибертероризъм-заплаха-отвъд-вирту/ (last access 11.06.2016); Мале, П. Заплахата от кибертероризма придобива очертания. http://e-vestnik.bg/16797/zaplahata-ot-kiberterorizma-pridobiva-ochertaniya/ (last access 11.06.2016).

[14] See: Deloitte - India Banking Fraud Survey - Edition II, 2015, p. 13.

The major type of damage suffered by banks due to breaches of data security relate to: [15]

- *Direct financial losses* due to theft of funds held and managed by the commercial bank;
- *Indirect financial losses* due to regulatory fines, legal costs, recovery and clean-up costs, loss of customer trust and loyalty;
- *Image (Reputation) costs* which relate to the loss of public and customer trust due to the public disclosure of data security breaches and leakage of confidential information about bank transactions, customers, money laundering, involvement in criminal schemes, etc.
- *Opportunity costs* due to accidents with data security within a bank which, in addition to the two items above, also refer to the deteriorating competitiveness of a bank; shifts in internal and organizational priorities; reduced workload which affects operating profit, etc.;
- *IT Defense costs* which include costs for designing IT and communication infrastructure to prevent attacks and ensure the fault tolerance of bank IT systems, as well as costs related to the deployment of organizational measures to increase data security and to improve the training and awareness of staff and customers in terms of newly emerging IT risks and their prevention.

Managers of commercial banks have a crucial role in the process of managing data security within the overall process of operational risks

[15] Adapted and supplemented after: Lagazio, M., Sherif, N., Cushman, M. A multi-level approach to understanding the impact of cyber crime on the financial sector. p. 11-12.

management.[16] Hence, the *Board of Directors* has the responsibility to design and develop an operational framework for managing the risk related to data security; to determine the maximum tolerance of the institution to this type of risk; and to ensure adequate capital to secure the risk which the bank takes. The operational framework may be approached as a set of policies and strategies adopted by banks in the sphere of data security; the methods that banks employ to identify, assess and minimize risk, as well as their organizational structure, powers, and responsibilities in terms of risk management. [17]

The role *of senior bank management* in this process relates to establishing the prerequisites for the efficient introduction and implementation of the policies, strategies, and procedures which the Board has prescribed and approved for managing the risk related to data security, as well as its direct responsibilities in terms of general management, assessment and monitoring of the overall process and the implementation of corrective actions in case of identified deficiencies and omissions, or changes in the internal and/or external environment.

Some of the measures adopted to increase data security also relate to the recruitment and training of bank officers; upgrading the hardware and software products which banks use; as well as the implementation of efficient internal control policies.

[16] For further reading on issues related to the management of bank risks, see: Божинов, Б. Управление на рисковете в търговската банка. Библиотека „Образование и наука“, бр. 58, АИ „Ценов“, Свищов, 2013.

[17] For further reading on issues related to bank policies, see: Божинов, Б. Актуални аспекти на банковата политика. Библиотека „Образование и наука“, бр. 50, АИ „Ценов“, Свищов, 2013.

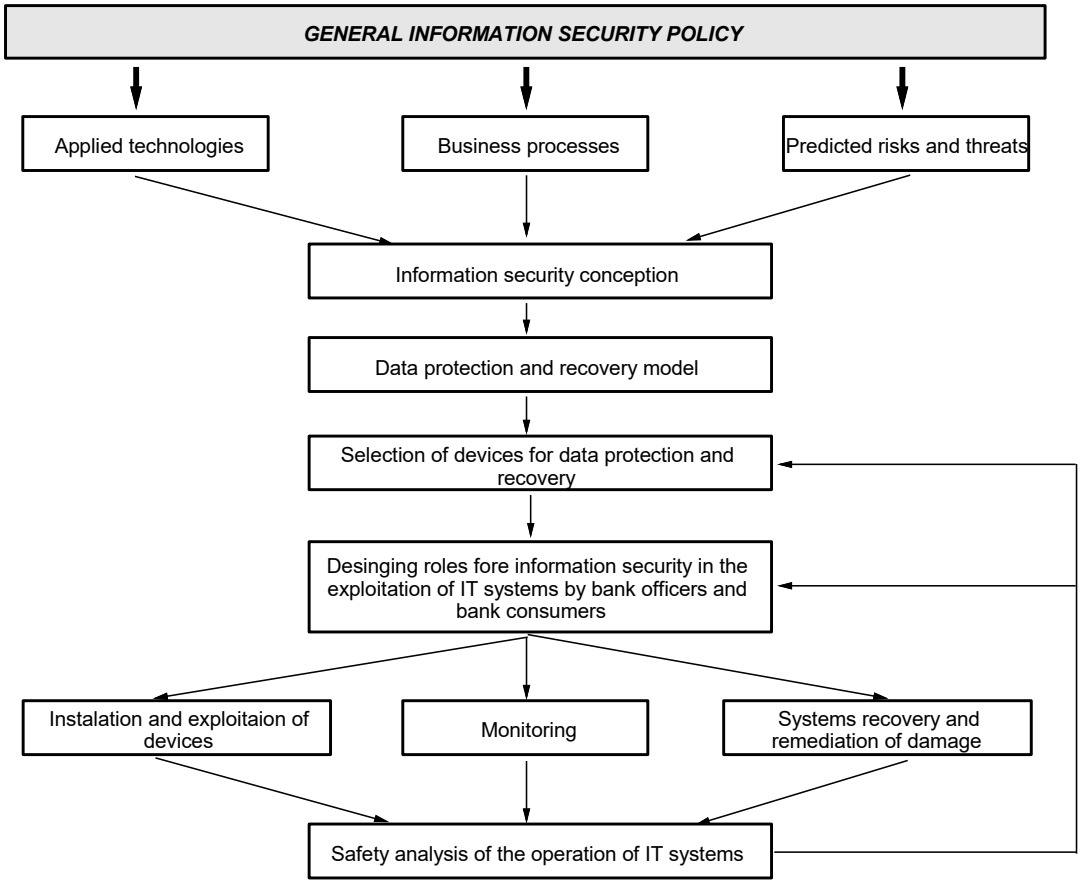

Fig. 3. Principle technology for ensuring data security at commercial banks[18]

The operational management of the risk related to data security is usually the responsibility of specialized information security units which may report directly to IT departments or to Risk Management Committees. Direct supervision on the activity of bank employees by their line managers in terms of compliance with established rules and procedures for internal control is, of course, an important condition for reducing the risk of internal bank fraud and omissions.

[18] See: Тютюнник А.В., Турбанов А.В. Банковское дело. Финансы и статистика, Москва, 2005, с. 458.

Inasmuch as the risk related to data security belongs to the category of the so called ‘pure risks’, i.e. it may only incur losses, the major approaches related to its management refer to:

- *Risk aversion* – this approach is only applicable to certain aspects of the risk which banks are able to avoid (for example, by refusing to provide remote banking);
- *Risk taking by providing reserves* which may be statutory (for example, in compliance with Ordinance No. 8 of the Bulgarian National Bank) or voluntary;
- *Risk transferring to third parties*, including through insurance, hiring outside providers of IT services, and any other applicable methods;
- *Risk minimization through assessment*; adequate procedures for process management, reporting, and efficient internal control; recruitment, training and qualification of bank employees;
- *Risk diversification* (only applicable to certain aspects of operational risk, mainly related to systems and software) by introducing mechanisms to back up exploited technological, technical, and communication solutions; outside providers of services; alternative methods for providing services, etc.

The fast rate of development of IT and communication technology and the advent of hi-tech innovations in all spheres of human life force banks to identify adequate tools for the operational management and minimization of risks related to their data security. Some of the latest approaches in this aspect include the deployment of multi-factor

authentication; geo-location; device recognition; cross channels to monitor and analyze user behavior, etc. [19]

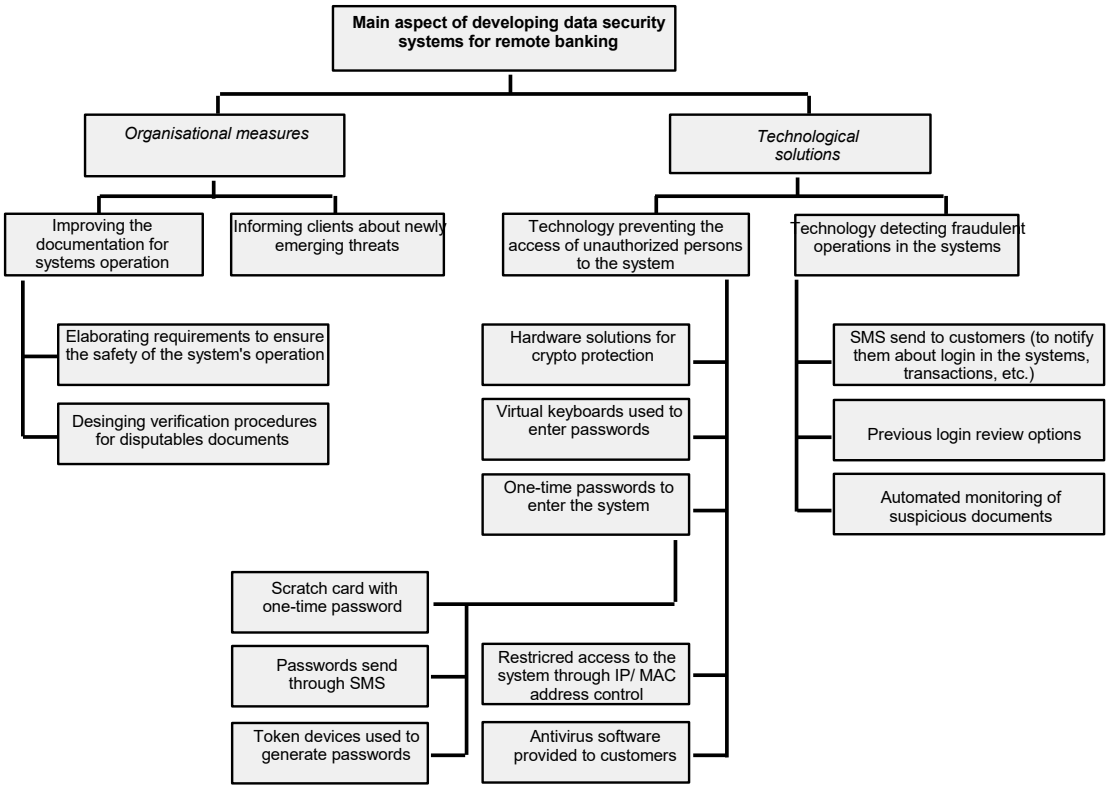

Fig. 4. Major aspects of improving information security with remote banking[20]

Multi-factor authentication relates to the deployment of a multi-step process for unique user identification in which, in addition to standard user names and passwords, various devices and methods are used alongside some private information provided by bank clients during the account opening phase (such as their favorite football team, the brand of their first car, their pets, etc.) so that they could be uniquely recognized by banks' automated IT systems. As for the *devices and equipment* which banks employ for user authentication, in most cases these are tokens

[19] See: ACI Univercal Payment. Fighting online fraud: an industry perspective. volume 3, 2014, p. 5-6.

[20] See: Визгунов, А., Визгунов, Ар. Уровень защищенности от несанкционорованного доступа как ключевой показатель качества системь дистанционного банковского обслуживания. Информационнье технологии в бизнесе, Бизнес-информатика, №2(12), 2010, с. 39.

which generate random numbers; USB devices containing login credentials or other unique information; notifications delivered as text messages (including about sending a single confirmation code).

Banks have recently started using the MAC addresses of their customers' devices (computers, tablets, telephones) and geo-location services (through IP addresses or GPS) to assess the potential risk of conducted transactions and to request further information for the unique identification of ordering parties in transactions. Furthermore, automated expert systems are increasingly introduced by banks to analyze consumer behavior (for example, the usual time they log in, their typical actions, the typical amount, frequency, direction and means of payment, the devices they use) and thus detect any irregularities (the so called 'red flags') which indicate a potential fraud attempt, including through identity theft.

Over the last years, banks have started integrating 'disaster recovery plans' into their data security management policies. Those plans include measures for identifying and designing alternative mechanisms and channels to resume their services in case they are interrupted (through back-up equipment, technology, communication links, emergency power systems, etc.); designing backup systems ensuring quick recovery of data archives at minimum or no loss of data (building clusters, applying virtualization systems, real time data duplication, high backup frequency to ensure minimum loss of data) and creating Disaster Recovery centers including by using external providers or cloud services.

* * *

Conclusion

Globalization and digitization processes have been altering slowly, yet irreversibly all aspects of contemporary society. While providing new opportunities and facilities, these processes also pose new risks and challenges, hence the growing importance of data and data security in the new digital environment. The only available solution for commercial banks is to adapt to and evolve in the new circumstances, which requires digitization and automation of existing processes; exploitation of new distribution channels to offer bank products and services; as well as creating new products and services. Hence, data security risk management has become a new key aspect of bank risk management and the overall management of bank establishments.

References

1. Алавердов А.Р. Организация и управление безопасностью в кредитно-финансовых организациях. Московская финансово-промышленная академия. Москва, 2004.

2. Божинов, Б. Актуални аспекти на банковата политика. Библиотека „Образование и наука“, бр. 50, АИ „Ценов“, Свищов, 2013.

3. Божинов, Б. Банковата сигурност – основни проявления и аспекти. Народностопански архив, бр. 3, 2016.

4. Божинов, Б. Управление на рисковете в търговската банка. Библиотека „Образование и наука“, бр. 58, АИ „Ценов“, Свищов, 2013.

5. Визгунов, А., Визгунов, Ар. Уровень защищенности от несанкционированного доступа как ключевой показатель качества системь дистанционного банковского обслуживания. Информационнье технологии в бизнесе, Бизнес-информатика, №2 (12), 2010.

6. Димитрова, Т. Вътрешният одит – ефективен инструмент на банковия мениджмънт, библиотека Образование и наука, бр. 38, АИ Ценов, Свищов, 2013.

7. Звезда, И.И. К вопросу о классификации способов мошенничества в банковской сфере. Известия Тульского государственного университета. Экономические и юридические науки, 2015, том 3-2, 97-105.

8. Лаврушин, О.И. Банковский менеджмент. Москва, Кронус, 2009.

9. Трифонова, С. Управление на операционния риск на банките. Вътрешен одитор, VII, N 1, 2010.

10. Тютюнник А.В., Турбанов А.В. Банковское дело. Финансы и статистика, Москва, 2005.

11. Шишманов, К. Използването на съвременните информационни технологии в банковото дело - предизвикателство и реалност. // Финансова стабилизация и икономически растеж: Международна научно-практическа конференция, Свищов, 2000, с. 119-122.

12. Шишманов, К. Рисковете при използването на интернет банкирането и отговорността на потребителите . // Финансите и стопанската отчетност - състояние, тенденции, перспективи : Юбилейна международна научнопрактическа конференция, Сборник доклади, Т. 1., Свищов , 2013, с. 79-84.

13. ACI Univercal Payment. Fighting online fraud: an industry perspective. volume 3, 2014.

14. Batiz-Lazo, B., Wood, D. Information technology innovations and commercial banking: a review and appraisal from an historical perspective. Accounting and finance research unit, Manchester Business School, The University of Manchester, 2001.

15. Deloitte - India Banking Fraud Survey - Edition II, 2015.

16. Dictionary of Banking and Finance. A&C Black Publishers Ltd, 2005.

17. Financial Fraud Action UK. News release

18. Fitch, T. Dictionary of Banking terms. Barrons's, 1997.

19. Lagazio, M., Sherif, N., Cushman, M. A multi-level Approach to understanding the Impact of Cyber Crime on the Financial Sector.

20. Storm, A. Establishing The Link Between Money Laundering And Tax Evasion. The Clute Institute International Academic Conference Munich, Germany 2014.

Internet Sources

21. Кибертероризъм – заплаха отвъд виртуалното пространство. http://news.unabg.org/кибертероризъм-заплаха-отвъд-вирту/ (last access 11.06.2016).

22. Мале, П. Заплахата от кибертероризма придобива очертания. http://e-vestnik.bg/16797/zaplahata-ot-kiberterorizma-pridobiva-ochertaniya/ (last access 11.06.2016).

23. Хакери атакуваха сайта на гръцката централна банка. http://news.bnt.bg/bg/a/khakeri-atakuvakha-sayta-na-grtskata-tsentralna-banka (last access 29.05.2016).

24. Хакери източили $71 млн. от банка през SWIFT. http://technews.bg/article-90580.html (last access 29.05.2016).

25. Хакери са източвали средства от близо 100 банки по света. http://www.capital.bg/biznes/kompanii/2015/02/16/2473701_hakeri_sa_iztochvali_sredstva_ot_blizo_100_banki_po/ (last access 29.05. 2016).

26. Alacer. Happy Birthday, Anti Money Laundering! http://www.alacergroup.com/happy-birthday-anti-money-laundering/ (last access 11.6.2016).